

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Brian C. Barnes, et al

Serial No.: 09/901,531

Filed: July 9, 2001

For: SOFTWARE MODEM WITH HIDDEN
AUTHENTICATION COMMANDS

Confirmation No.: 7123

Examiner: C. Brown

Group Art Unit: 2134

Att'y Docket: 2000.054600

Customer No. 023720

APPEAL BRIEF

Mail Stop Appeal Brief – Patents

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby submit this Appeal Brief to the Board of Patent Appeals and Interferences in response to the Final Office Action dated June 16, 2006.

The Assistant Commissioner is authorized to deduct the fee for filing this Appeal Brief (\$500.00) and any other fees required under 37 C.F.R. §§ 1.16 to 1.21 from the Williams, Morgan & Amerson, P.C. Deposit Account No. 50 0786/2000.054600.

TABLE OF CONTENTS

SECTION	PAGE
I. REAL PARTY IN INTEREST	3
II. RELATED APPEALS AND INTERFERENCES	3
III. STATUS OF THE CLAIMS	3
IV. STATUS OF AMENDMENTS	3
V. SUMMARY OF CLAIMED SUBJECT MATTER	3
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	7
VII. ARGUMENT	7
VIII. CLAIMS APPENDIX	11
IX. EVIDENCE APPENDIX	11
X. RELATED PROCEEDINGS APPENDIX	12
XI. CONCLUSION	12
APPENDIX (CLAIMS AT ISSUE)	13

I. REAL PARTY IN INTEREST

Advanced Micro Devices, Inc., the assignee hereof, is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences of which Applicants, Applicants' legal representative, or the Assignee is aware of that will directly affect or be directly affected by or have a bearing on the decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-21 are pending in the case. The Final Office Action rejected claims 1-4, 6-15, and 7-21. Claims 5 and 16 were deemed allowable, but were objected to as being dependent from a rejected parent claim.

IV. STATUS OF AMENDMENTS

All previous amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to Figure 1, a block diagram of a communications system 10 is provided. The communications system 10 includes a user station 20 in communication with a central station 30 over a communication channel 40. In the illustrated embodiment, the user station 20 is a mobile computing device using a software modem 50 to communicate in accordance with a wireless communication protocol, such as GSM. The central station 30 may be a shared base station capable of serving a plurality of subscribers. The user station 20 may comprise a variety of computing devices, such as a desktop computer, a notebook computer, a personal data assistant (PDA), etc. For purposes of illustration, the user station 20 is described as it may be implemented using a notebook computer. The software modem 50 may be installed as an internal resource. As will be appreciated by those of ordinary skill in the art, the software modem 50 includes a physical layer (PHY) 70 implemented in hardware and a protocol layer 80 implemented in software. For purposes of illustration, the functions of the software modem 50 are described as they might be implemented for a GSM communication protocol, although other protocols may be used.

The PHY layer 70 converts digital transmit signals into an analog transmit waveform and converts an incoming analog received waveform into digital received signals. For transmit signals, the output signal of the protocol layer 80 is the transmit “on-air” information modulated about a zero Hz carrier (*i.e.*, a carrierless signal). The PHY layer 70 mixes (*i.e.*, mixing may also be referred to as upconverting) the carrierless transmit signal generated by the protocol layer 80 in accordance with assigned time slot, frequency, and power level assignments communicated to the user station 20 by the central station 30 to generate the actual analog waveform transmitted by the PHY layer 70. The central station 30 also communicates time slot and frequency assignments to the user station 20 for incoming data. The incoming analog receive waveform is sampled and downconverted based on the assigned time slot and frequency parameters to recreate a carrierless (*i.e.*, modulated about zero Hz) receive waveform. The protocol layer 80 receives the carrierless receive waveform from the PHY layer 70 and performs baseband processing, decryption, and decoding to regenerate the received data. Collectively, the time slot, frequency, and power level (*i.e.*, for transmit data only) assignments are referred to as control codes.

The data received by the protocol layer 80 is encrypted. The functions of the protocol layer 80 include decoding and decrypting the received data, extracting the control codes and user data, and sending the control codes to the PHY layer 70. The commands sent to the PHY layer 70 by the protocol layer 80 include a hidden authentication command. If the authentication command is missing or does not coincide with what is expected by the PHY layer 70, the PHY layer 70 inhibits further operation of the modem 50.

The modem driver 240 decrypts the received encrypted data and decodes the decrypted data to extract control codes and/or user data. The modem driver determines an authentication code based on the control codes after they are extracted. The specific construct of the authentication code may vary. For example, the authentication code may be a mathematical combination of the control code values or a binary manipulation of the bits making up the values (*i.e.*, similar to a checksum). Alternatively, the modem driver 240 may encrypt the control codes based on a secret key provided by the vendor and stored in a secure location (*e.g.*, in the system BIOS 170 or in a secure storage device on the ACR card 215). After determining and storing the authentication code, the modem driver 240 stores the extracted control codes for transfer to the PHY hardware 220.

The modem driver 240 passes the control codes to the PHY hardware 220. Coincident with the command that includes the control codes, the modem driver also sends the authentication code in such a way that is hidden or hard to detect for a hacker trying to co-opt the modem driver 240. Because the authentication code is hidden, the hacker may try to modify the control codes without realizing that the authentication code exists. The PHY hardware 220 is adapted to recognize the inconsistency between the altered control codes and the authentication code and prevent the radio 230 from being operated. If no inconsistency between the control codes and the authentication code exists, the PHY hardware 220 accepts the control codes and configures the radio 230 based on the assigned time slot, frequency, and power level information contained in the control codes.

Exemplary techniques for hiding the authentication code from normal detection include embedding the authentication code in normally unused bits on a data bus or by embedding the authentication code in unused and normally ignored data frames. Sending the authentication code in a portion of the data communication framework that is normally unused or ignored is generically referred to herein as sending the authentication code “out-of-band.”

Thus, with respect to claim 1, a communications system (10), the invention comprises:

- a physical layer hardware unit (220) adapted to communicate data over a communications channel (40) in accordance with assigned transmission parameters, the physical layer hardware unit (220) being adapted to receive an incoming signal over the communications channel (40) and sample the incoming signal to generate a digital received signal; and
- a processing unit (100) adapted to execute a software driver (240) including program instructions adapted to extract control codes from the digital received signal, generate an authentication code, and transfer the control codes and the authentication code to the physical layer hardware unit (220), wherein the physical layer hardware unit (220) is adapted to signal a security violation in response to the control codes being inconsistent with the authentication code.

With respect to claim 12, a method for identifying security violations in a transceiver (50), the invention comprises:

- receiving digital data over a communications channel (40);
- extracting control codes from the digital received signal;
- generating an authentication code based on at least one extracted control code;
- transferring the control codes and the authentication code to a physical layer hardware unit (220) of the transceiver (50);
- configuring assigned transmission parameters of the physical layer hardware unit (220) based on the control codes; and
- signaling a security violation in response to the control codes being inconsistent with the authentication code.

With respect to claim 21, a modem, the invention comprises:

- means for receiving digital data over a communications channel (40);
- means for extracting control codes from the digital received signal;
- means for generating an authentication code based on at least one extracted control code;
- means for transferring the control codes and the authentication code to a physical layer hardware unit (220) of the modem;
- means for configuring assigned transmission parameters of the physical layer hardware unit (220) based on the control codes; and
- means for signaling a security violation in response to the control codes being inconsistent with the authentication code.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Are claims 1, 7-12, and 18-21 obvious under 35 U.S.C. § 103(a) over Roeck (U.S. Patent No. 6,594,305) in view of Nay (U.S. Patent No. 5,237,567)?

B. Are claims 2-3 and 13-14 obvious under 35 U.S.C. § 103(a) over Roeck and Nay in further view of Spelman (U.S. Patent No. 5,680,458)?

C. Are claims 4 and 15 obvious under 35 U.S.C. § 103(a) over Roeck and Nay in further view of Mergard (U.S. Patent No. 5,881,248)?

D. Are claims 6 and 17 obvious under 35 U.S.C. § 103(a) over Roeck and Nay in further view of Whitmire (U.S. Patent No. 6,115,817)?

VII. ARGUMENT

A. THE COMBINATION OF ROECK AND NAY FAILS TO OBTAIN ANY CLAIM.

The claimed subject matter, as set forth in independent claims 1, 12, and 21, includes the general features of Applicants receiving digital data over a communications channel, extracting control codes from the digital received signal, generating an authentication code based on at least one extracted control code, transferring the control codes and the authentication code to a physical layer hardware unit of the transceiver, configuring assigned transmission parameters of the physical layer hardware unit based on the control codes, and signaling a security violation in response to the control codes being inconsistent with the authentication code.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an

obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. The combination of Roeck and Nay fails to meet these criteria for a *prima facie* case of obviousness for several reasons.

First, the combination of Roeck and Nay fails to teach every element of the claimed invention. Roeck describes a ping protocol for determining whether a link in a network system utilizing cable modems is operational regardless of a modem's registration status. See Roeck, col. 1, lines 15-20. However, as admitted by the Examiner, Roeck is completely silent with regard to the use of authentication codes or determining security violations. The Examiner therefore alleges that Nay describes generating an authentication code. Applicants respectfully disagree. Nay describes using parity bits, check bits, and/or checksums for error detection and/or correction. See Nay, col. 37, lines 35-62. Nay is completely silent with regard to any type of authentication technique or determining whether or not a security violation has occurred. Nay fails to address security, only data transmission accuracy. A system constructed by combining Roeck and Nay would simply attempt to correct a transmission error if the received data did not match the checksum using known ECC techniques or request the data be transmitted again. This is similar to what modems implementing ECC code already do with data received over the communication channel. Data errors are not classified as security violations. Identifying a data transmission error simply does not equate to identifying a security violation.

In the Final Office Action, the Examiner maintains that Nay describes generating an authentication code by equating a data transfer error checking code to a security related authentication code. Applicants respectfully disagree with this construction. The Office Action indicates that Nay discovers errors in data transmission using a checksum. Even if assuming, solely for the sake of argument, that the checksum of Nay equates to an authentication code, Nay still fails to signal a security violation in response to the checksum not matching the sent data. If Nay detects a problem, the data is corrected automatically using the ECC data or resent. Nay

does not detect a security violation, because Nay does not contemplate that the data may be tampered with, but rather only that the data was not received properly. The Office Action asserts that a violation in Nay could be the result of tampering and, hence, the data error of Nay equates to a security violation. The Office Action fails to support this possibility based on the teachings of Nay, but rather just based on an ungrounded conclusory statement. One significant defect in this construction is that it completely ignores the effect of the “security” modifier to the violation term. As admitted by the Office Action Nay only looks at data integrity, regardless of the source of a data error. If Nay detects an error in the sent data, the data is corrected or resent and no violation of any kind is identified, much less a security violation.

Second, Applicants submit that the cited references also fail to provide any suggestion or motivation for modifying the prior art of record to arrive at the claimed invention. As discussed above and as admitted by the Examiner, Roeck is completely silent with regard to the use of authentication codes or determining security violations. Moreover, as discussed above, Roeck is concerned with determining whether a link in a network system utilizing cable modems is operational regardless of a modem’s registration status. Thus, Roeck is unconcerned with performing any authentication of the cable modem and consequently provides no suggestion or motivation to modify the prior art to incorporate any authentication techniques in the manner suggested by the Examiner. Nay is concerned with detecting and/or correcting errors that occur during transmission of data over a bus. Thus, Nay is unconcerned with authentication and consequently provides no suggestion or motivation to modify the prior art to incorporate any authentication techniques in the manner suggested by the Examiner.

In the Advisory Action, the examiner admits that the grounds for combining Roeck and Nay are not grounded in the art themselves, but rather based on the Examiner’s assessment of the level of knowledge of one of ordinary skill in the art. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35. With respect to alleged obviousness, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the

absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997).

As grounds for combining Roeck and Nay, the Examiner states “It would be obvious to combine the communication system of Roeck with the authentication mechanism of Nay to prevent message tampering and improve security. In the Final Office Action , the Examiner further states, “[O]ne of ordinary skill in the art would recognize both the benefit and motivation to use the method of insuring data integrity, and prevent errors to secure a system and make it reliable.” This statement supports Applicant’s position that Nay is concerned only with data integrity for reliability purposes, not security purposes. As neither Roeck nor Nay is directed to preventing message tampering or improving security, the only grounds for such a combination arise from an improper use of Applicant’s disclosure as a roadmap.

Because the combination of Roeck and Nay fails to teach each and every element of the claimed invention, and the Office has failed to meet its burden of providing motivation to combine Roeck and Nay based on grounds found in the prior art, the *prima facie* case of obviousness is deficient. Accordingly, claims 1, 12, 21, and all claims depending therefrom are allowable. Applicants respectfully request the rejection of these claims be reversed.

B. THE COMBINATION OF ROECK, NAY, AND SPELMEN FAILS TO OBLIVIATE ANY CLAIM.

Claims 2, 3, 13, and 14 are allowable for at least the reasons provided above for claims 1, 12, and 21. Spelman fails to correct the primary defects identified with Roeck and Nay. In rejecting claims 2, 3, 13, and 14 over Roeck and Nay in further view of Spelman, the Office Action suggests that it would be obvious to provide the Roeck-Nay system with out-of-band messaging to assure that the message has not been tampered with. The grounds for establishing combinability must be found in the prior art. Because Roeck and Nay are completely silent regarding identifying security violations, but rather only data transmission errors, it is inconceivable that grounds could be found in Roeck or Nay to combine Spelman therewith. Nay would have no reason to send the checksum out-of-band with respect to the data, as data and checksums are conventionally always provided over the same channel. This combination constitutes an impermissible use of hindsight using Applicants’ disclosure as a roadmap. For

these additional reasons, claims 2, 3, 13, and 14 are themselves allowable, and Applicants respectfully request the rejection of these claims be reversed.

C. THE COMBINATION OF ROECK, NAY, AND MERGARD FAILS TO OBVIATE ANY CLAIM.

Claims 4 and 15 are allowable for at least the reasons provided above for claims 1, 12 and 21. Mergard fails to correct the primary defects identified with Roeck and Nay. In rejecting claims 4 and 15 in further view of Mergard, the Office Action suggest that it would be obvious to send the authentication code out-of-band and over an unused portion of the bus to improve bus performance. Again, Nay would have no reason to send the checksum out-of-band with respect to the data as data and checksums are conventionally always provided over the same channel. The authentication code is not sent out-of-band to improve bus performance, but rather to send the authentication code separately from the control codes to increase the difficulty that a malicious entity might have in identifying the authentication code. Again, this combination constitutes an impermissible use of hindsight using Applicants' disclosure as a roadmap. For these additional reasons, claims 4 and 15 are themselves allowable and Applicants respectfully request the rejection of these claims be reversed.

D. THE COMBINATION OF ROECK, NAY, AND WHITMIRE FAILS TO OBVIATE ANY CLAIM.

Claims 6 and 17 are allowable for at least the reasons provided above for claims 1 and 12. The Whitmire fails to correct the primary defects identified with Roeck and Nay. Applicants respectfully request the rejection of these claims be reversed.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

The rejections fail because the cited art of record fails to teach all the limitations of the claims and the grounds for combining Roeck and Nay cannot be supported. More particularly, the art of record fails to teach or suggest generating an authentication code based on at least one extracted control code, transferring the control codes and the authentication code to a physical layer hardware unit of a transceiver, configuring assigned transmission parameters of the physical layer hardware unit based on the control codes, and signaling a security violation in response to the control codes being inconsistent with the authentication code. Applicants therefore pray that the rejections be reversed and the claims be allowed to issue.

Respectfully submitted,

Date: August 3, 2006

/Scott F. Diring/

Scott F. Diring
Reg. No. 35,119
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-4070
(713) 934-7011 (Fax)

ATTORNEY FOR APPLICANTS

APPENDIX
(Claims at Issue)

1. (Previously Presented) A communications system, comprising:
 - a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal; and
 - a processing unit adapted to execute a software driver including program instructions adapted to extract control codes from the digital received signal, generate an authentication code based on at least one extracted control code, and transfer the control codes and the authentication code to the physical layer hardware unit, wherein the physical layer hardware unit is adapted to signal a security violation in response to the control codes being inconsistent with the authentication code.
2. (Original) The system of claim 1, wherein the authentication code comprises a hidden authentication code.
3. (Original) The system of claim 1, wherein the software driver includes program instructions adapted to transfer the authentication code out-of-band with respect to the control codes.
4. (Original) The system of claim 3, wherein the processor complex includes a data bus, and the software driver includes program instructions adapted to transfer the authentication code on an unused portion of the data bus.
5. (Original) The system of claim 3, wherein the processing unit includes a data bus adapted to transfer data in frames having a fixed number of slots, and the software driver includes program instructions adapted to transfer the authentication code using a frame having more slots than the fixed number of slots.

6. (Original) The system of claim 1, wherein the software driver includes program instructions adapted to extract encrypted data from the digital received signal and decrypt the encrypted data to generate decrypted data including the control codes.

7. (Original) The system of claim 6, wherein the software driver includes program instructions adapted to generate the authentication code based on the decrypted data.

8. (Original) The system of claim 1, wherein the assigned transmission parameters include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

9. (Original) The system of claim 1, wherein the processing unit comprises a computer.

10. (Original) The system of claim 9, wherein the computer includes:
a processor complex adapted to execute the program instructions in the software driver;
a bus coupled to the processor complex; and
an expansion card coupled to the bus, the expansion card including the physical layer hardware.

11. (Original) The system of claim 1, wherein the physical layer hardware unit is adapted to prohibit at least some communication over the communications channel in response to identifying the security violation.

12. (Previously Presented) A method for identifying security violations in a transceiver, comprising:

- receiving digital data over a communications channel;
- extracting control codes from the digital received signal;
- generating an authentication code based on at least one extracted control code;
- transferring the control codes and the authentication code to a physical layer hardware unit of the transceiver;
- configuring assigned transmission parameters of the physical layer hardware unit based on the control codes; and
- signaling a security violation in response to the control codes being inconsistent with the authentication code.

13. (Original) The method of claim 12, wherein generating the authentication code further comprises generating a hidden authentication code.

14. (Original) The method of claim 12, wherein transferring the control codes and the authentication code comprises transferring the authentication code out-of-band with respect to the control codes.

15. (Original) The method of claim 14, wherein transferring the control codes and the authentication code comprises transferring the authentication code on an unused portion of a data bus communicating with the transceiver.

16. (Original) The method of claim 14, wherein the transceiver is coupled to data bus adapted to transfer data in frames having a fixed number of slots, and transferring the control codes and the authentication code comprises transferring the authentication code using a frame having more slots than the fixed number of slots.

17. (Original) The method of claim 12, further comprising:
extracting encrypted data from the digital received signal; and
decrypting the encrypted data to generate decrypted data including the control codes.

18. (Original) The method of claim 17, wherein generating the authentication code comprises generating the authentication code based on the decrypted data.

19. (Original) The method of claim 12, wherein configuring assigned transmission parameters of the physical layer hardware unit based on the control codes comprises configuring at least one of a power level parameter, a frequency parameter, and a time slot parameter.

20. (Original) The method of claim 12, further comprising prohibiting communication over the communications channel in response to identifying the security violation.

21. (Previously Presented) A modem, comprising:
means for receiving digital data over a communications channel;
means for extracting control codes from the digital received signal;
means for generating an authentication code based on at least one extracted control code;
means for transferring the control codes and the authentication code to a physical layer hardware unit of the modem;
means for means for configuring assigned transmission parameters of the physical layer hardware unit based on the control codes; and
means for signaling a security violation in response to the control codes being inconsistent with the authentication code.